Device-independent verifiable blind quantum computation

Michal Hajdušek,[1,*] Carlos A. Pérez-Delgado,[1,†] and Joseph F. Fitzsimons[1,2,‡]

[1] *Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

As progress on experimental quantum processors continues to advance, the problem of verifying the correct operation of such devices is becoming a pressing concern. The recent discovery of protocols for verifying computation performed by entangled but non-communicating quantum processors holds the promise of certifying the correctness of arbitrary quantum computations in a fully device-independent manner. Unfortunately, all known schemes have prohibitive overhead, with resources scaling as extremely high degree polynomials in the number of gates constituting the computation. Here we present a novel approach based on a combination of verified blind quantum computation and Bell state self-testing. This approach has dramatically reduced overhead, with resources scaling as only $O(m^4 \ln m)$ in the number of gates.

In recent years, significant progress has been made on the development of quantum information processing technologies. Basic operations with fidelities exceeding those required for fault-tolerant quantum computation have already been demonstrated in both ion-traps [1, 2] and superconducting systems [3]. The number of qubits available in a single device is also approaching the limit of our ability to fully characterize the device, due to the exponential growth in the size of the state space. Quantum algorithms running on large scale quantum computers hold the promise of dramatic reductions in run time for certain problems. However, as the size of a quantum processor begins to exceed our ability to fully characterize it, the question of whether one can trust results produced in this manner naturally arises. For certain problems, such as integer factorization via Shor's algorithm [4], the results of the computation can be verified efficiently by a classical computer. However, this property does not extend to a number of important problems such as the simulation of chemistry and other quantum systems [5].

While there is currently no known way to verify a single adversarial quantum processor, two distinct approaches have begun to emerge to the problem of verifying quantum processors based on interrogation performed during computation. In the first approach, a quantum processor is repeatedly queried by some other smaller quantum device, generally of fixed size, which can be characterized by conventional means. Aharonov, Ben-Or and Eban introduced an approach to such quantum prover interactive proofs based on quantum authentication using a fixed-sized quantum processor for the verifier [6]. An alternative route to verification is based on the universal blind quantum computation (UBQC) protocol of Broadbent, Fitzsimons and Kashefi [7], which provides an unconditionally secure [8] protocol for hiding quantum computations delegated to a remote server. By constructing the delegated computation to include certain *traps* it is possible to verify that the computation has been performed correctly, with exponentially small probability of error [9, 10]. These protocols have extremely modest requirements for the verifier, simply the ability to prepare or measure single qubits in a finite set of bases. As such, it has proven possible to implement blind computation [11] and verification [12] in a system of four photonic qubits.

The second approach to verification is based on the interrogation of two or more entangled but non-communicating quantum processors. Reichardt, Unger and Vazirani [13] showed that arbitrary quantum processing could be verified entirely classically utilizing the statistics of CHSH games [14]. McKague [15] discovered an alternative approach using entangled processors based on measurement-based computation, through a self-testing protocol for certain graph states.

These two approaches have complimentary strengths and weaknesses. The second approach provides a stronger security guarantee, since the prohibition on communication between processors can be enforced through space-like separation of the devices. This removes the need for the verifier to place trust in any pre-existing device, no matter how simple, and can be said to be truly device independent: if the tests are passed, the verifier can be confident in the result of the computation even if quantum devices were constructed by an adversary, without need for any characterization. However the known protocols are only efficient in the theoretical sense, the required resources scale as an extremely high degree polynomial of the circuit dimensions. On the other hand, approaches to verification based on blind computation are characterized by far better resource scaling, with overhead scaling as low as linearly in the circuit size. Here we present a hybrid approach, in which self-testing is used to prepare the initial resource for verifiable blind computation, and then the computation is implemented using an existing blind computation scheme. The resulting protocol is entirely device independent, while requiring resources many orders of magnitude less than existing protocols.

Results

Before explaining our results it would be useful to discuss what is meant by verifying a quantum computation. A verification protocol is such where a single verifier interacts with one or more provers. The verifier accepts at the end of the

*Electronic address: michal˙hajdusek@sutd.edu.sg
†Electronic address: carlos.perez@quantumlah.org
‡Electronic address: joseph˙fitzsimons@sutd.edu.sg

protocol if the output is correct, and should reject otherwise. More formally, we say that a protocol with a quantum operator input U and a classical output to be correct if the output is a possible result of measuring the state $U|0\rangle$ in the Pauli-X basis. Following Definition 10 in [9], given any $0 \leq \omega < 1$, a protocol is ω-verifiable if for any choice of the prover's strategy the probability p_{error} of the verifier accepting an incorrect outcome is bounded by ω, $p_{error} \leq \omega$.

When purely classical output is required, several blind quantum computation protocols [7, 9, 16] have the property that they can be decomposed into two phases: an initial state distribution phase, where direct quantum communication is used to prepare a fixed classical-quantum (CQ) correlation between the verifier's classical system and the quantum processor to be tested, followed by an execution phase during which purely classical communication is used to implement and verify the computation. Our approach is to replace the first phase of an existing verification protocol, namely Protocol 6 introduced in [9], with an alternate method of creating the same correlation which admits a self-testing strategy. The second phase of the protocol remains unaltered, and so security is guaranteed if the initial state can be prepared with sufficiently high fidelity.

Protocol 6 of [9] uses a cylindrical brickwork state as a resource. A vertex is randomly chosen to be a trap qubit. The rest of the qubits in the row containing this trap and the qubits in either the lower or the upper row, depending which is connected to the trap qubit, are prepared in eigenstates of the computational basis. This effectively disentangles the trap qubit from the rest of the resource state which now acts as the usual brickwork state originally used to achieve UBQC. Because the trap qubit is separated from the rest of the state, the client has a finite probability of detecting a cheating server.

Our remote state preparation procedure is inspired by a two-device variant of the UBQC protocol [7, 17, 18]. Rather than directly transmitting a quantum state from the verifier to the server, measurements on one half of an entangled pair shared between two devices are used to project the remote system in a particular basis, thereby generating the desired correlations. We will assume that the verifier's device consists of a simple measurement device capable of measuring individual qubits in an arbitrary basis, inspired by the blind computation approach taken by Morimae and Fujii [19], where Bob sends the resource to Alice one qubit at a time and she performs the computation using her device which effectively hides the computation from a malicious Bob. We also require that Bob's subsystems are spatially separated such that measurements on all of them can be performed in a space-like separated manner, and that they be spatially arranged such that this separation is apparent to Alice. We will treat the quantum part of the verifier's device and the quantum processor to be verified as (potentially collaborating but non-communicating) adversaries, yielding a situation in which there is a purely classical verifier and $N+1$ quantum provers. Alice's quantum measuring device is considered one of the provers while the remaining N are in Bob's possession and each of them sequentially sends an EPR pair to be measured by Alice's device. This sequential transmission needs to occur in a sufficiently short time period that all meaurements required by the protocol can be made while respecting spacelike separation between the measurement events for each prover. We shall refer to the verifier as Alice and the quantum device to be verified as Bob, with the distinction between the quantum and classical systems of Alice clear from context. We retain the terminology of the single prover setting, since, due to the asymmetry of the provers, it is natural to think of our approach as a blind quantum computing protocol in which Alice self-tests her own device.

At each step of phase one, Alice will receive a qubit from Bob. She chooses randomly to either use that qubit for verification purposes, or for the purpose of helping remotely create the resource state that will be used in phase two. The two procedures can be intuitively thought of, and are best analysed, as two distinct protocols. However it is crucial to keep in mind that the two protocols are randomly interwoven and executed in the same phase. This ensures that Bob has no knowledge about which qubits are used for self-testing and which for remote state preparation.

The self-testing procedure compares two experiments. The reference experiment consists of a multipartite state $|\psi\rangle_Q$ on Hilbert space Q and local observable T_{Q_j}, where j labels the subsystem. The physical experiment consists of a multipartite state $|\psi\rangle_S$ on Hilbert space S and local observable T_{S_j}. In order to self-test operations and states with complex coefficients we also require Hilbert space R, which is used to determine that the devices either both apply the desired operator or they both apply its complex conjugate. The physical experiment is said to be ε-equivalent to the reference experiment if there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$, such that

$$\left\| \Phi\left(T_{S_j}|\psi\rangle_S\right) - \frac{1}{\sqrt{2}}\left(|junk_1\rangle_S \otimes T_{Q_j}|\psi\rangle_Q|00\rangle_R + |junk_2\rangle_S \otimes T^*_{Q_j}|\psi\rangle_Q|11\rangle_R\right)\right\|_2 \leq \varepsilon,$$

where $\|\cdot\|_2$ is the vector distance defined for two vectors $|a\rangle$ and $|b\rangle$ as $\||a\rangle - |b\rangle\|_2 = \sqrt{(\langle a| - \langle b|)(|a\rangle - |b\rangle)}$, and $T^*_{Q_j}$ is the complex conjugate of T_{Q_j}. The state $|junk\rangle_S \otimes T_{Q_j}|\psi\rangle_Q$ represents the ideal state up to local isometry.

At every step of phase one, Bob is asked to prepare a Bell pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and send half of it to Alice. She will measure the received qubit in a randomly chosen basis $\alpha \in \{X_A, Y_A, Z_A, D_A, E_A^{\pm}, F_A\}$, where X_A, Y_A, Z_A are Pauli operators, $D_A = \frac{1}{\sqrt{2}}(X_A + Z_A)$, $E_A^{\pm} = \frac{1}{\sqrt{2}}(\pm X_A + Y_A)$ and $F_A = \frac{1}{\sqrt{2}}(Y_A + Z_A)$. Here we use $Y_A = Y$ and $Y_B = -Y$. After Alice measures all of her qubits, she requests Bob to measure all, except m randomly chosen qubits, of his qubits in random basis $\beta \in \{X_B, Y_B, Z_B\}$ and send her the result. Since the state that is being verified is symmetric, Alice does not need to test $Y_A X_B$, $Z_A X_B$, or $Z_A Y_B$. Furthermore, measurement settings $D_A Y_B$, $E_A^+ Z_B$, $E_A^- Z_B$, $F_A X_B$ are not necessary in our analysis. There are in total 14 measurement settings that are required in our self-testing analysis.

Alice collects all measurement results and at the end of phase one she performs a statistical verification, deciding whether, with some confidence p, every single one of the

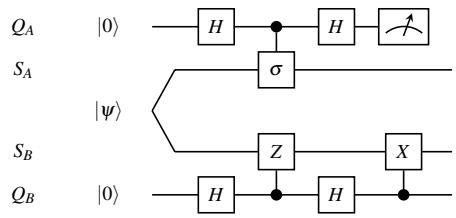

FIG. 1. Local isometry Φ used to identify the ideal state in Bob's device. The isometry is a reduced swap gate acting individually on Bob's subsystem and we can think of Φ as extracting the desired state using the measured statistics.

qubits she received were part of a state $\tilde{\varepsilon}$-close to a Bell pair. If this is the case, she proceeds to phase two. The verification protocol used in this phase is based on the approach of Mayers and Yao in [20, 21], which was greatly simplified and further developed by McKague *et al.* in [22, 23]. This does not require a trusted measurement device, and can be tailored for any security parameters p and ε.

The graph state generation proceeds similarly to the UBQC protocol [7, 9]. However, instead of Alice sending a prepared qubit to Bob, Alice measures her half of the Bell pair in order to collapse Bob's half of the pair to one of the valid input states. Specifically, the verification protocol for classical inputs and outputs which we will make use of (Protocol 6 of [9]), requires Alice to prepare and send to Bob, for each qubit $1 \leq j \leq m$ needed in the computation stage, a state $|\psi_j\rangle$ chosen uniformly at random either from the set $\{|0\rangle, |1\rangle\}$ or the set $\left\{|+_{\theta_j}\rangle\right\}_{\theta_j \in A}$, where $|+_{\theta_j}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta_j}|1\rangle\right)$ and $A = \{0, \pi/4, \ldots, 7\pi/4\}$. Here, instead of directly preparing the state $|\psi_j\rangle$, Alice instructs her measurement device to measure her half of the Bell pair in the basis $\{|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\}$, where $|-_{\theta_j}\rangle = |+_{\theta_j+\pi}\rangle$, if she wants to prepare a qubit in the $x-y$ plane, and in the computational basis if she wants to prepare a dummy qubit. If she measures her half to be in the state $|+_{\theta_j}\rangle$, then she knows that Bob's state is (with high probability) in the state $|+_{-\theta_j}\rangle$. Similarly, if she measures $|-_{\theta_j}\rangle$, then she knows that Bob's half is in the state $|-_{-\theta_j}\rangle$. The case of measurements in the computational basis is even simpler. If Alice measures $|s\rangle$, where $s \in \{0,1\}$, then Bob's qubit will be prepared in the same state. Since Alice does not announce the angle θ_j, and since the outcome of her measurement is uniformly random, Bob has no information about the input state. The state that they share is given by a CQ correlation [7], with Alice holding a classical label for Bob' state, given by $\frac{1}{2}\sum_{s\in\{0,1\}} |s\rangle\langle s|_A \otimes |s\rangle\langle s|_B$ for dummy qubits and $\frac{1}{8}\sum_{\theta_j \in A} |\theta_j\rangle\langle\theta_j|_A \otimes |+_{-\theta_j}\rangle\langle+_{-\theta_j}|_B$ for qubits used in computation. Tracing out Alice's subsystem reveals that Bob's state is maximally mixed.

Unlike many self-testing schemes, our goal is not to certify that Alice and Bob share an EPR pair up to a local isometry. Instead we use the measured statistics to certify that for a given measurement outcome on Alice's device, Bob is in possession of a state close to the ideal corresponding state up to a local isometry. This is pictured in Fig. 1 for measurements with only real coefficients and in Fig. 3 for measurements with complex complex coefficients.

Protocol 1 Device-Independent Remote State Preparation

Input: Security parameters p and ε, and constant $c \geq 1$.

Steps:

1. Alice initialises counters $k^{\alpha\beta} = 0$ and a correlation estimator $\hat{C}^{\alpha\beta} = 0$ for all α and β. She randomly partitions the $N = m + 14c\tilde{n}$ qubits that she will receive from Bob into m qubits to be used for input preparation, and $N-m$ qubits to be used for verification from which she will randomly draw $\tilde{n}$ qubits per measurement setting.
2. For $1 \leq i \leq N$
   (a) Bob is asked to prepare a Bell pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and sends one half to Alice.
   (b) If the received qubit is for verification, then
      i. Alice randomly chooses an observable α and an observable β, and increments the counter $k^{\alpha\beta}$.
      ii. Alice measures her state according to α, recording the outcome $a^{\alpha\beta}_{k^{\alpha\beta}} \in \{-1, 1\}$.
      iii. Alice instructs Bob to measure his qubit according to β.
      iv. Bob measures his half of the prepared Bell pair in the instructed basis, and sends his result $b^{\alpha\beta}_{k^{\alpha\beta}} \in \{-1, 1\}$ to Alice.
      v. Alice updates her correlation estimator for this particular measurement setting $\hat{C}^{\alpha\beta} = \frac{1}{k^{\alpha\beta}}\left[(k^{\alpha\beta}-1)\hat{C}^{\alpha\beta} + a^{\alpha\beta}_{k^{\alpha\beta}} \cdot b^{\alpha\beta}_{k^{\alpha\beta}}\right]$.
   (c) If the received qubit is for remote state preparation, then
      i. Alice measures her half of the Bell pair in the basis $\{|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\}$, where θ_j is chosen uniformly at random from A, if Bob's corresponding qubit is to be used for computation or for trap preparation. If his qubit is to be used for dummy qubit preparation, Alice measures in $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$.
      ii. If Alice's measurement outcome is $|+_{\theta_j}\rangle$, then Bob's input qubit is $|+_{-\theta_j}\rangle$, whereas if her measurement outcome is $|-_{\theta_j}\rangle$, then Bob's input qubit is $|-_{-\theta_j}\rangle$. If, instead, Alice measures in the computational basis and the outcome is $|s\rangle$, where $s \in \{0,1\}$, then Bob's input qubit is $|s\rangle$. Alice stores a classical label for Bob's state in memory.
3. If $\left(1-\exp\left(-(\tilde{n}+m)\varepsilon^2/8\right)\right)^3 \left(1-2\exp\left(-(\tilde{n}+m)\varepsilon^2/8\right)\right)^{11} \geq p$, and $|\hat{C}^{\alpha\beta} - \mu^{\alpha\beta}| \leq \varepsilon$, for all α and β, and $\mu^{\alpha\beta}$ is the value of ideal correlation for a particular α and β, then the protocol succeeds, otherwise it aborts. Alice also aborts if she does not gather enough statistics about a certain subset of correlations. The probability of this occurring decreases exponentially with increasing c.

Protocol 1 shows how Alice can remotely prepare single qubit states in Bob's subsystem, up to isometry, without revealing such states to Bob and in a completely device-independent manner. The following theorem shows the cor-

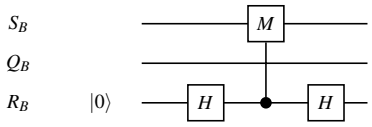

FIG. 2. Isometry Φ' used to obtain information about complex operations applied by Bob.

rectness of the protocol. That is, unless Alice aborts the protocol, Bob will be in possession, with probability at least p, of qubit states $\tilde{\varepsilon}$-close to the ideal state.

Theorem 1. *Let $|\psi\rangle$ be the untrusted state shared by Alice and Bob. Given a projection $\Pi^{\pm}_{\sigma_A}$ corresponding to the result of Alice's measurement of σ_A and that the measured correlations in Protocol 1 are χ-close to the ideal correlations, there exists a local isometry $\bar{\Phi}$ that extracts a state close to the desired state on Bob's side,*

$$\Big\| \bar{\Phi}\left(\sqrt{2}\Pi^{\pm}_{\sigma_{S_A}}|\psi\rangle_S\right) - \Big[(I+M_{S_A})|junk_\sigma\rangle_S \Pi^{\pm}_{Z_{Q_A}} \Pi^{\pm}_{\sigma_{Q_B}}|\phi^+\rangle_Q|0\rangle_R + (I-M_{S_B})|junk_\sigma\rangle_S \Pi^{\pm}_{Z_{Q_A}} \left(\Pi^{\pm}_{\sigma_{Q_B}}\right)^* |\phi^+\rangle_Q|1\rangle_R\Big]\Big\|_2 \leq \tilde{\varepsilon},$$

where $\tilde{\varepsilon} = O(\chi^{1/4})$.

Proof. We start with an outline of the main idea behind the proof. By considering the behaviour of the devices as given by the gathered statistics, we show that the operators applied by the devices on the untrusted state $|\psi\rangle$ must follow commutation and anti-commutation relations close to the ideal Pauli operators applied on the ideal shared state $|\phi^+\rangle$, provided that the measured statistics are close to the ideal statistics. Next we construct a local isometry $\bar{\Phi} = \Phi \circ \Phi'$, composed of a reduced swap operation Φ and a phase-kickback operation Φ'. The local isometry $\bar{\Phi}$ captures the fact that the statistics remain unchanged under local change of basis, addition of ancillae, change of the action of the observables outside of the support of the state, and local embedding of the observables and states in a different Hilbert space. Using the correlations shared by the untrusted devices, we show that $\bar{\Phi}$ extracts a state close to the desired ideal one. The role of the phase-kickback Φ' is to distinguish when the operations of the devices are complex conjugated.

The first step uses a result obtained by McKague *et al.* in [22] which establishes a bound on the maximum distance between an untrusted shared state and an ideal Bell pair, up to local isometry, given statistics for correlations of measurements $\{X_A, Z_A, D_A\}$ on Alice's subsystem and $\{X_B, Z_B\}$ on Bob's subsystem. By extending this approach to include measurements with complex coefficients we obtain the maximum distance between the state that Alice's measurement remotely prepares on Bob's subsystem and the ideal input state. Assume the real correlations are all at most χ-far from the ideal case. This means that the actual correlations satisfy $\langle\psi|X_AX_B|\psi\rangle \geq 1-\chi$, $\langle\psi|Z_AZ_B|\psi\rangle \geq 1-\chi$, $|\langle\psi|X_AZ_B|\psi\rangle| \leq \chi$, $|\langle\psi|D_AX_B|\psi\rangle - \frac{1}{\sqrt{2}}| \leq \chi$, $|\langle\psi|D_AZ_B|\psi\rangle - \frac{1}{\sqrt{2}}| \leq \chi$ with

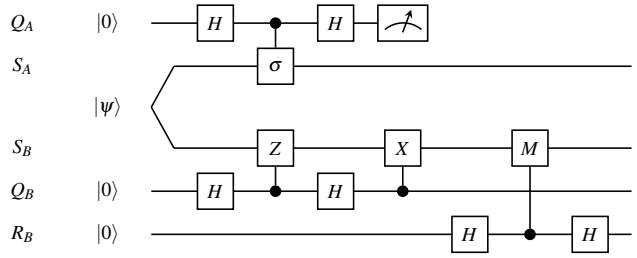

FIG. 3. The total local isometry $\bar{\Phi} = \Phi' \circ \Phi$ used in the self-testing analysis of gathered statistics. Alice performs a measurement of the observable σ. The isometry $\bar{\Phi}$ extracts the corresponding state on Bob's side as well as the information about the complex phase of the applied measurement.

high probability. This leads to bounds on the action of the measured observables,

$$\begin{aligned}
\|(X_AZ_A + Z_AX_A)|\psi\rangle\|_2 &\leq 2\varepsilon_1, && \text{(1a)}\\
\|(X_BZ_B + Z_BX_B)|\psi\rangle\|_2 &\leq 2\varepsilon_1 - 4\varepsilon_2, && \text{(1b)}\\
\|(X_A - X_B)|\psi\rangle\|_2 &\leq \varepsilon_2, && \text{(1c)}\\
\|(Z_A - Z_B)|\psi\rangle\|_2 &\leq \varepsilon_2, && \text{(1d)}
\end{aligned}$$

where $\varepsilon_1 = (1+\sqrt{2})\sqrt{(1+2\sqrt{2})\chi + \sqrt{2\chi}} + 2\sqrt{2\chi}$ and $\varepsilon_2 = \sqrt{2\chi}$. Similar inequalities can be derived also for Y_A and Y_B using the corresponding correlations such as $\langle\psi|Y_AY_B|\psi\rangle$.

Bounds in Eq. (1c) and Eq. (1d) can be obtained by using the definition of the vector norm and using the fact that measurements of X_AX_B and Z_AZ_B are both nearly correlated. Bounds on the anti-commutation of the measurement operators on the same subsystem in Eq. (1a) and Eq. (1b) require more work. First, it can be shown from $|\langle\psi|X_AZ_B|\psi\rangle| \leq \chi$ that $X_B|\psi\rangle$ and $Z_B|\psi\rangle$ are nearly orthogonal and similarly for Alice's subsytem. This in turn leads to a nearly unitary operator $\frac{1}{\sqrt{2}}(X_B + Z_B)$ which can be used to obtain Eq. (1b). Details of this derivation can be found in Appendix C in [22].

Now we will discuss how the isometry $\bar{\Phi}$, presented in FIG. 3, extracts the desired state and information about the complex phase of the measurements. This approach is based on a technique first introduced by McKague and Mosca in [23]. Alice's measurement projects the shared state in register S to $\sqrt{2}\Pi^{\pm}_{\sigma_{S_A}}|\psi\rangle_S$, where $\Pi^{\pm}_{\sigma_{S_A}} = \frac{1}{2}(I \pm \sigma_{S_A})$ is the corresponding projector. For an outcome a of Alice's measurement, the isometry can be expressed as

$$\begin{aligned}
\bar{\Phi}\left(\sqrt{2}\Pi^{\pm}_{\sigma_{S_A}}|\psi\rangle_S\right) &= \frac{1}{4\sqrt{2}} \sum_{k,l\in\{0,1\}} \left(I + (-1)^l M_{S_B}\right)\\
&\times X^k_{S_B}\left(I + (-1)^k Z_{S_B}\right) \qquad (2)\\
&\times (I + (-1)^a \sigma_{S_A})\,|\psi\rangle_S |ak\rangle_Q |l\rangle_{R_B}.
\end{aligned}$$

The action of this isometry is two-fold. The first part of the isometry, Φ depicted in FIG. 1, swaps the states in registers S_B and Q_B. The second part of the isometry, Φ' shown in FIG. 2, requires a third register on Bob's side, denoted by R_B. The

effect of this second part is to extract information about the complex phase of the applied measurement.

The isometry Φ' does not affect the state of the register Q_B when Alice measures in basis X_A or Z_A. In particular, by substituting these bases into Eq. (2) and considering the ideal case when $\chi = 0$ in Eq. (1), we see that the states transform as $\sqrt{2}\Pi^{\pm}_{X_{S_A}}|\psi\rangle_S \to |junk_X\rangle_S 2\Pi^{\pm}_{Z_{Q_A}}\Pi^{\pm}_{X_{Q_B}}|\phi^+\rangle_Q$ and $\sqrt{2}\Pi^{\pm}_{Z_{S_A}}|\psi\rangle_S \to |junk_Z\rangle_S 2\Pi^{\pm}_{Z_{Q_A}}\Pi^{\pm}_{Z_{Q_B}}|\phi^+\rangle_Q$, where we do not care about the state of the register S after the isometry. Using the fact that Y_A anti-commutes with X_A and Z_A (we are still considering the case when $\chi = 0$), we can establish that $Y_A \to Y_{Q_A}M_{S_A}$, where M_{S_A} is a unitary and similarly for Y_B. This means that in the ideal case, for any measurement that Alice performs, we have

$$\begin{aligned}&\bar{\Phi}\left(\sqrt{2}\Pi^{\pm}_{\sigma_{S_A}}|\psi\rangle_S\right)\\ &= \frac{1}{2}\left[(I+M_B)|junk_\sigma\rangle_S\frac{1}{\sqrt{p_\sigma}}\Pi^{\pm}_{Z_{Q_A}}\Pi^{\pm}_{\sigma_{Q_B}}|\phi^+\rangle_Q|0\rangle_{R_B}\right. \quad (3)\\ &\left.+(I-M_B)|junk_\sigma\rangle_S\frac{1}{\sqrt{p_\sigma}}\Pi^{\pm}_{Z_{Q_A}}\left(\Pi^{\pm}_{\sigma_{Q_B}}\right)^*|\phi^+\rangle_Q|1\rangle_{R_B}\right],\end{aligned}$$

where $p_\sigma = \langle\phi^+|\Pi^{\pm}_{Z_{Q_A}}\Pi^{\pm}_{\sigma_{Q_A}}|\phi^+\rangle$. This shows that the register Q_B contains the ideal desired state corresponding to Alice's measurement and the complex phase of the measurement is controlled on the state of register R_B.

Finally, we can consider the case when $\chi \neq 0$. By comparing Eq. (2) with Eq. (3), along with the bounds in Eq. (1) and repeated application of triangle inequality as in Appendix A of [22], we obtain that the distance between the real state and the ideal state, up to some local isometry, is at most $\tilde{\varepsilon} = \frac{1}{2}(9\varepsilon_1 + \varepsilon_2)$. □

What remains to be shown is the scaling of Alice's confidence about Bob's state given the gathered statistics from self-testing. We forgo the use of a Chernoff bound as this would require the assumption of independent behaviour and would compromise device-independence. Rather we adopt a similar approach to Pironio *et al.* [24]. The measurement process forms a martingale with bounded increment which allows the application of Azuma-Hoeffding inequality [25, 26].

Denote the set of all EPR pairs that Alice and Bob share by $\mathscr{S}$ with cardinality $|\mathscr{S}| = N$. This set can be partitioned into the subset of pairs used in self-testing that are measured by both Alice and Bob, $\mathscr{S}_{\text{test}} \subset \mathscr{S}$ with $|\mathscr{S}_{\text{test}}| = n$, and the set of pairs used for remote state preparation where only Alice measures her subsystems, $\mathscr{S}_{\text{prep}} \subset \mathscr{S}$ with $|\mathscr{S}_{\text{prep}}| = m$. We also have $N = n + m$.

Consider an arbitrary subset $\tilde{\mathscr{S}} \subseteq \mathscr{S}$ that is again partitioned as above, $\tilde{\mathscr{S}} = \tilde{\mathscr{S}}_{\text{test}} \cup \tilde{\mathscr{S}}_{\text{prep}}$ with corresponding cardinalities $|\tilde{\mathscr{S}}| = \tilde{n} + \tilde{m}$. We can further partition the subset of pairs used in self-testing according to the basis that the qubits are measured in, $\tilde{\mathscr{S}}_{\text{test}} = \cup_{\alpha,\beta}\tilde{\mathscr{S}}^{\alpha\beta}_{\text{test}}$ with $\tilde{n} = \sum_{\alpha,\beta}\tilde{n}^{\alpha\beta}$, where $\tilde{\mathscr{S}}^{\alpha\beta}_{\text{test}}$ is the subset of pairs where Alice measures in α basis and Bob measures in β basis. Similarly we can partition $\tilde{\mathscr{S}}_{\text{prep}} = \cup_{\alpha,\beta}\tilde{\mathscr{S}}^{\alpha\beta}_{\text{prep}}$ with $\tilde{m} = \sum_{\alpha,\beta}\tilde{m}^{\alpha\beta}$. This may look strange at first since we have stated that $\tilde{\mathscr{S}}_{\text{prep}}$ is the subset of EPR pairs that get measured only on Alice's side. However, in the upcoming theorem, it is useful to consider hypothetical measurements in basis β by Bob.

The average ideal correlation over the subset $\tilde{S}$ can be written as

$$\tilde{\mu} = \frac{1}{|\tilde{\mathscr{S}}|}\sum_{\alpha,\beta}(\tilde{n}^{\alpha\beta} + \tilde{m}^{\alpha\beta})\tilde{\mu}^{\alpha\beta},$$

where $\tilde{\mu}^{\alpha\beta} = \langle\phi^+|\alpha\otimes\beta|\phi^+\rangle$ is the ideal correlation for a pair measured in α by Alice and β by Bob. Denoting the classical outcome of Alice's and Bob's measurement on the i^{th} pair by $a_i \in \{-1,1\}$ and $b_i \in \{-1,1\}$, respectively, we can define a random variable $\hat{C}_i = a_i b_i$. The average measured correlation over the subset $\tilde{\mathscr{S}}$ is then

$$\begin{aligned}\frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}}\hat{C}_i &= \frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}_{\text{test}}}\hat{C}_i + \frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}_{\text{prep}}}\hat{C}_i\\ &= \frac{1}{|\tilde{\mathscr{S}}|}\sum_{\alpha,\beta}\tilde{n}^{\alpha\beta}\left(\tilde{\mu}^{\alpha\beta} \pm \varepsilon^{\alpha\beta}\right) \quad (4)\\ &+ \frac{1}{|\tilde{\mathscr{S}}|}\sum_{\alpha,\beta}\tilde{m}^{\alpha\beta}\left(\tilde{\mu}^{\alpha\beta} \pm \varepsilon'^{\alpha\beta}\right),\end{aligned}$$

where $\varepsilon^{\alpha\beta}$ represents the measured deviation from ideal correlation for measurement $\alpha\beta$. For simplicity we set $\varepsilon^{\alpha\beta} = \varepsilon$ for all α,β. $\varepsilon'^{\alpha\beta}$ is the hypothetical deviation from ideal correlation obtained if Bob measured his qubits of $\tilde{\mathscr{S}}_{\text{prep}}$ as well. Since these qubits are in reality not measured we assume the worst case scenario,

$$\tilde{\varepsilon}'^{\alpha\beta} = \begin{cases} -2 & \text{when} \quad \tilde{\mu}^{\alpha\beta} = 1\\ -\left(1+\frac{1}{\sqrt{2}}\right) & \text{when} \quad \tilde{\mu}^{\alpha\beta} = \frac{1}{\sqrt{2}}\\ 1 & \text{when} \quad \tilde{\mu}^{\alpha\beta} = 0\\ 1+\frac{1}{\sqrt{2}} & \text{when} \quad \tilde{\mu}^{\alpha\beta} = -\frac{1}{\sqrt{2}}.\end{cases} \quad (5)$$

Again to simplify the notation we assume the most pessimistic scenario and set $|\varepsilon'^{\alpha\beta}| = 2$ for all α,β. The real correlation that the devices share is denoted by $C_i(W_A) = \Pr(a_i = b_i|W_A) - \Pr(a_i \neq b_i|W_A)$, where W_A denotes the history of Alice's instructions and measurements. The following theorem bounds the probability that the real average correlation deviates from the average ideal correlation by a large amount given the statistics from Alice's and Bob's measurements.

Theorem 2. *Given an arbitrary subset of EPR pairs, $\tilde{\mathscr{S}} \subseteq \mathscr{S}$, and that the measured average correlation is $\tilde{\mu} \pm \varepsilon$, the probability that the real average correlation over this subset is close to the ideal average correlation is given by*

$$Pr\left(\left|\frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}}C_i(W_A) - \tilde{\mu}\right| \leq \frac{2\tilde{n}\varepsilon + m(2+\varepsilon)}{\tilde{n}+m}\right) \geq 1 - 2\delta, \quad (6)$$

where $\delta = \exp(-(\tilde{n}+m)\varepsilon^2/8)$.

Proof. We first look at the case when the measured average correlation is $\tilde{\mu} + \varepsilon$. Define a new random variable,

$$Y_k = \sum_{i=1}^{k}\left[C_i(W_A) - \hat{C}_i\right],$$

where $k \in \{0,1,\ldots,|\tilde{\mathscr{S}}|\}$. The expected value of $|Y_n|$ is finite and the conditional expected value is $E(Y_{k+1}|W_A) = Y_k$. Also the random variable has a bounded increment, $c_k = |Y_{k+1} - Y_k| \leq 2$ for all k. Therefore the random variable Y_k is a martingale with bounded increment an so we can apply the Azuma-Hoeffding inequality

$$\Pr\left(Y_{|\tilde{\mathscr{S}}|} \geq \gamma\right) \leq \exp\left(-\frac{\gamma^2}{2\sum_{i\in\tilde{\mathscr{S}}} c_i^2}\right). \tag{7}$$

Choosing $\gamma = |\tilde{S}|\varepsilon$, Eq. (7) can rewritten as

$$\Pr\left(\frac{1}{|\tilde{\mathscr{S}}|}\left[\sum_{i\in\tilde{\mathscr{S}}} C_i(W_A) - \sum_{i\in\tilde{\mathscr{S}}} \hat{C}_i\right] \geq \varepsilon\right) \leq \exp\left(-\frac{1}{8}|\tilde{\mathscr{S}}|\varepsilon^2\right).$$

Splitting the expression for the measured average correlation as in Eq. (4) and assuming the worst case scenario, $\varepsilon'^{\alpha\beta} = 2$, we get

$$\begin{aligned}\Pr\left(\frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}} C_i(W_A) - \tilde{\mu} \;\geq\; \frac{2\tilde{n}\varepsilon + \tilde{m}(2+\varepsilon)}{|\tilde{\mathscr{S}}|}\right) \\ \leq\; \exp\left(-\frac{1}{8}|\tilde{\mathscr{S}}|\varepsilon^2\right)\end{aligned} \tag{8}$$

Defining the martingale as $Y_k = \sum_{i=1}^{k}\left[\hat{C}_i - C_i(W_A)\right]$, and following the same steps as above we arrive at a new bound,

$$\Pr\left(\frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}} C_i(W_A) - \tilde{\mu} \leq \frac{\tilde{m}(2-\varepsilon)}{|\tilde{\mathscr{S}}|}\right) \leq \exp\left(-\frac{1}{8}|\tilde{\mathscr{S}}|\varepsilon^2\right). \tag{9}$$

Combining Eq. (8) with Eq. (9), the probability that the average real correlation is close to the average ideal correlation is

$$\begin{aligned}&\Pr\left(\frac{\tilde{m}(2-\varepsilon)}{|\tilde{\mathscr{S}}|} \leq \frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}} C_i(W_A) - \tilde{\mu} \leq \frac{2\tilde{n}\varepsilon + \tilde{m}(2+\varepsilon)}{|\tilde{\mathscr{S}}|}\right) \\ &\geq 1 - 2\exp\left(-\frac{1}{8}|\tilde{\mathscr{S}}|\varepsilon^2\right).\end{aligned} \tag{10}$$

The lower endpoint of the interval in Eq. (10) can be extended while keeping the same lower bound on the probability,

$$\begin{aligned}&\Pr\left(\left|\frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}} C_i(W_A) - \tilde{\mu}\right| \leq \frac{2\tilde{n}\varepsilon + \tilde{m}(2+\varepsilon)}{|\tilde{\mathscr{S}}|}\right) \\ &\geq 1 - 2\exp\left(-\frac{1}{8}|\tilde{\mathscr{S}}|\varepsilon^2\right).\end{aligned}$$

Using $\tilde{m} \leq m$, we can extend the interval further

$$\Pr\left(\left|\frac{1}{|\tilde{\mathscr{S}}|}\sum_{i\in\tilde{\mathscr{S}}} C_i(W_A) - \tilde{\mu}\right| \leq \frac{2\tilde{n}\varepsilon + m(2+\varepsilon)}{\tilde{n}+m}\right) \geq 1 - 2\delta,$$

where $\delta = \exp\left(-(\tilde{n}+m)\varepsilon^2/8\right)$. Identical expression is obtained for the case when the average measured correlation is $\tilde{\mu} - \varepsilon$.

□

If we are interested in a particular correlation $\alpha\beta$, as in Theorem 1, we can obtain the appropriate bound and probability by setting $\tilde{\mathscr{S}}$ to include all the pairs that are measured in the basis $\alpha\beta$ and no other pairs where both Alice and Bob measure. Also we set $\chi = \frac{2\tilde{n}\varepsilon + m(2+\varepsilon)}{\tilde{n}+m}$ in this case. It can be seen that this is sufficient to imply Theorem 1 by considering an initial set of $\tilde{n}+m$ pairs, used to test a single correlation and then randomly inserting an additional $\tilde{n}$ qubits of each additional correlation to be tested. The tests are then always such that they can be considered to have been performed on subsets of cardinality $\tilde{n}+m$, where the location of the m untested qubits remains random.

Theorem 1 bounds the maximum distance between the ideal state, shared between Alice and Bob, which we denote $|\psi_j^{AB}\rangle$, and the actual state $|\phi_j^{AB}\rangle$ that they share, up to local isometry on Bob's side (since the classical labels are stored in Alice's classical memory rather than her quantum device). It is important to keep in mind that $|\psi_j^{AB}\rangle$ represents the ideal two-qubit state up to local isometry Φ. In other words, $|\psi_j^{AB}\rangle$ is not itself in general a two-qubit state, just as performing a partial trace of it over Alice's subsystem does not in general result in a single-qubit state on Bob's subsystem. For any fixed value of Alice's classical register the reduced state on Bob's side is pure, denoted by $|\psi_j^{B}\rangle$, provided he follows the protocol honestly. Expressing the distance between this ideal state and the state obtained from a run of the protocol, in which Bob is not constrained to be honest, in terms of the vector distance makes it straightforward to obtain a lower bound on the fidelity of Bob's input state. Infidelity, introduced into the input state by Bob's dishonest behaviour, leads to an additive error in the probability of the verification protocols of [9] accepting an incorrect outcome.

Each of the verification protocols considered in [9] can be viewed as a quantum channel $\mathscr{P}(\rho)$ which acts on a fixed CQ correlated state. The probability of accepting a state orthogonal to the output in the case of an honest run is then given by the expectation value of the projector $P_\perp$ onto the orthogonal but accepted subspace. The initial state of Bob's subsystem is $\rho^B = p\rho^B_{\leq\tilde{\varepsilon}} + (1-p)\rho^B_{>\tilde{\varepsilon}}$, where $p = (1-\delta)^3(1-2\delta)^{11}$ is the probability of preparing a state $\rho^B_{\leq\tilde{\varepsilon}}$ which is the result from Alice's measurement on her subsystem, where the bipartite system $|\phi_j^{AB}\rangle$ was $\tilde{\varepsilon}$-close in vector distance to the ideal state $|\psi_j^{AB}\rangle$ for all $j \in \{1,\ldots,m\}$. $\rho^B_{>\tilde{\varepsilon}}$ is defined in a similar fashion. The probability of accepting an incorrect outcome is given by

$$p_{\text{error}} = \text{Tr}\left(P_\perp \mathscr{P}(\rho^B)\right).$$

Substituting in the expression for ρ^B, p_{error} becomes a sum of three terms. The first term, $p\text{Tr}\left(P_\perp \mathscr{P}(|\psi^B\rangle\langle\psi^B|)\right)$, represents the probability that Alice accepts the incorrect output given the correct input. The second term, $p\text{Tr}\left(P_\perp \mathscr{P}(\rho^B_{\leq\tilde{\varepsilon}} - |\psi^B\rangle\langle\psi^B|)\right)$, provides a correction to the first term for a state $\tilde{\varepsilon}$-close to the correct input. Lastly, $(1-p)\text{Tr}\left(P_\perp \mathscr{P}(\rho^B_{>\tilde{\varepsilon}})\right)$ is the probability of accepting the wrong output given an input state that is more than $\tilde{\varepsilon}$-far from the correct input. Evaluating these expressions gives the final

Protocol 2 Device-Independent Blind Quantum Computation

Input: On Alice's side:

1. Security parameters p, ε and Δ.
2. A quantum computation expressed as a measurement based computation on a cylindrical brickwork state of m qubits, with measurement angles $\phi = (\phi_i)_{1\leq i\leq m}$ with $\phi_i \in A$, incorporating a set of trap qubits T and dummy qubits D chosen as described in the main text and illustrated in Figure 4.
3. m random variables θ_i with values taken uniformly at random from A.
4. A fixed function C_G that for each non-output qubit i computes the angle of the measurement to be sent to Bob. This function depends on $\phi_i, \theta_i, r_i, x_i$ and the result of the measurements that have been performed so far, $\mathbf{s}_{<i}$ (the definition of the function C_G is identical to the one found in [9], and its full description can be found there).

Steps:

1. Alice and Bob engage in Protocol 1.
2. Bob takes his m states prepared in the previous step and entangles them according to the cylindrical brickwork graph.
3. Alice sets all the values in $\mathbf{s}$ to be 0.
4. For $i:\ 1 \leq i \leq m$
   (a) Alice computes the angle $\delta_i = C_G(i, \phi_i, \theta_i, r_i, x_i, \mathbf{s})$ and sends it to Bob.
   (b) Bob measures qubit i with angle δ_i and sends Alice the result b_i.
   (c) Alice sets the value of s_i in $\mathbf{s}$ to be $b_i \oplus r_i$.
5. Alice accepts if $b_t = r_t$, for all traps $t \in T$.

bound on the probability of accepting an incorrect output,

$$p_{\text{error}} \leq p(1-\Delta) + p\|\rho^B_{\leq\tilde{\varepsilon}} - |\psi^B\rangle\langle\psi^B|\|_{\text{tr}} + (1-p),$$

where $1-\Delta$ is the maximum probability of accepting an incorrect outcome using the ideal initial state $|\psi^B\rangle$ and a multi-trap variant of the verification scheme in Protocol 6 in [9].

This concludes phase one of our protocol which tests the operation of Alice's device and produces a separable input state on Bob's quantum computer with high probability. Alice then proceeds with the computation by instructing Bob to entangle the prepared qubits into a graph state, and use that graph state to perform verifiable blind computation. The protocol they follow is given in Protocol 2, which is based on Protocol 6 in [9]. We have modified the protocol found there to have classical input and output only, and in order to make it device-independent. Correctness follows directly from the correctness of the unmodified protocol.

Protocol 6 of [9] uses a single qubit to detect Bob's deviation from Alice's instructions making the protocol $\left(1-\frac{1}{m}\right)$-verifiable. Alice randomly chooses a trap position t on a cylindrical brickwork state and prepares the rest of the qubits in the same and neigbouring row in computational basis turning them into dummy qubits. Instructing Bob to apply entangling operations according to the cylindrical brickwork graph blindly produces a rectangular brickwork state in a tensor product with a single trap that Alice uses for verification.

We modify this scheme to incorporate multiple trap qubits and obtain a protocol that is $(1-\Delta)$-verifiable, where $0 < \Delta < 1$ is a constant. Alice starts with a cylindrical brickwork state and chooses a set of trap qubits T, by randomly choosing a set R of consecutive rows and fixes a 2-colouring on the graph, taking all qubits in R of colour C are taken to be traps, as illustrated in Fig. 4. She prepares the remaining qubits located in the same rows as the trap qubits in the computational basis. Additionally Alice also prepares the qubits in rows located directly above and below R in the computational basis. We refer to the set of qubits containing the trap qubits and the dummy qubits prepared in the computational basis as a *tape*. Alice then instructs Bob to entangle the qubits according to the cylindrical brickwork graph which produces the brickwork state in a tensor product with $|T|$ trap qubits.

In order to achieve $(1-\Delta)$-verifiability for constant $\Delta < \frac{1}{2}$, we require that the width of the tape scales in such a way that $|R|$ is a constant fraction 2Δ of the total number of rows of the cylindrical brickwork state. The proof that this leads to a constant probability of accepting an incorrect outcome of the computation follows precisely the same steps as the proof of Theorem 8 in [9] which proves $\left(1-\frac{1}{m}\right)$-verifiability of a single-trap protocol, where the increased verifiability stems directly from the increased probability that any given qubit is a trap qubit. Correctness also follows directly from the correctness of Protocol 6 in [9]. Combining the multi-trap verification on cylindrical brickwork state with the self-testing procedure leads to the following corollary.

Corollary 1. *Protocol 2 is $(1-p\Delta+2p\sqrt{m}\tilde{\varepsilon})$-verifiable, that is the probability that an incorrect outcome is accepted at the end of the verification procedure is*

$$p_{error} \leq 1 - p\Delta + 2p\sqrt{m}\tilde{\varepsilon},$$

where $p \geq (1-\delta)^{3m}(1-2\delta)^{11m}$ is Alice's confidence that Bob is in possession of an m-qubit input state close to the ideal one, $\delta = \exp\left(-\frac{1}{8}\varepsilon^2(\tilde{n}+m)\right)$, and $\tilde{n}+m = O(m^4 \ln m)$ is the number of Bell pairs needed for self-testing per measurement setting.

Proof. Expanding the expression for the bound on the vector distance between the shared state and the ideal state up to isometry $\||\psi^{AB}_j\rangle - |\phi^{AB}_j\rangle\|_2 \leq \tilde{\varepsilon}$, for all j, we get $\text{Re}\langle\psi^{AB}_j|\phi^{AB}_j\rangle \geq 1 - \frac{1}{2}\tilde{\varepsilon}^2$, which can be used to obtain a lower bound on the fidelity between the states,

$$F(|\psi^{AB}_j\rangle, |\phi^{AB}_j\rangle) \geq \left(1 - \frac{1}{2}\tilde{\varepsilon}^2\right)^2,$$

where we used $F(|\psi^{AB}_j\rangle, |\phi^{AB}_j\rangle) = |\langle\psi^{AB}_j|\phi^{AB}_j\rangle|^2 \geq \text{Re}^2\langle\psi^{AB}_j|\phi^{AB}_j\rangle$. The fidelity is non-decreasing under partial trace which leads immediately to $F(|\psi^B_j\rangle, \rho^B_j) \geq (1 - \frac{1}{2}\tilde{\varepsilon}^2)^2$. Fidelity is also multiplicative under tensor products which

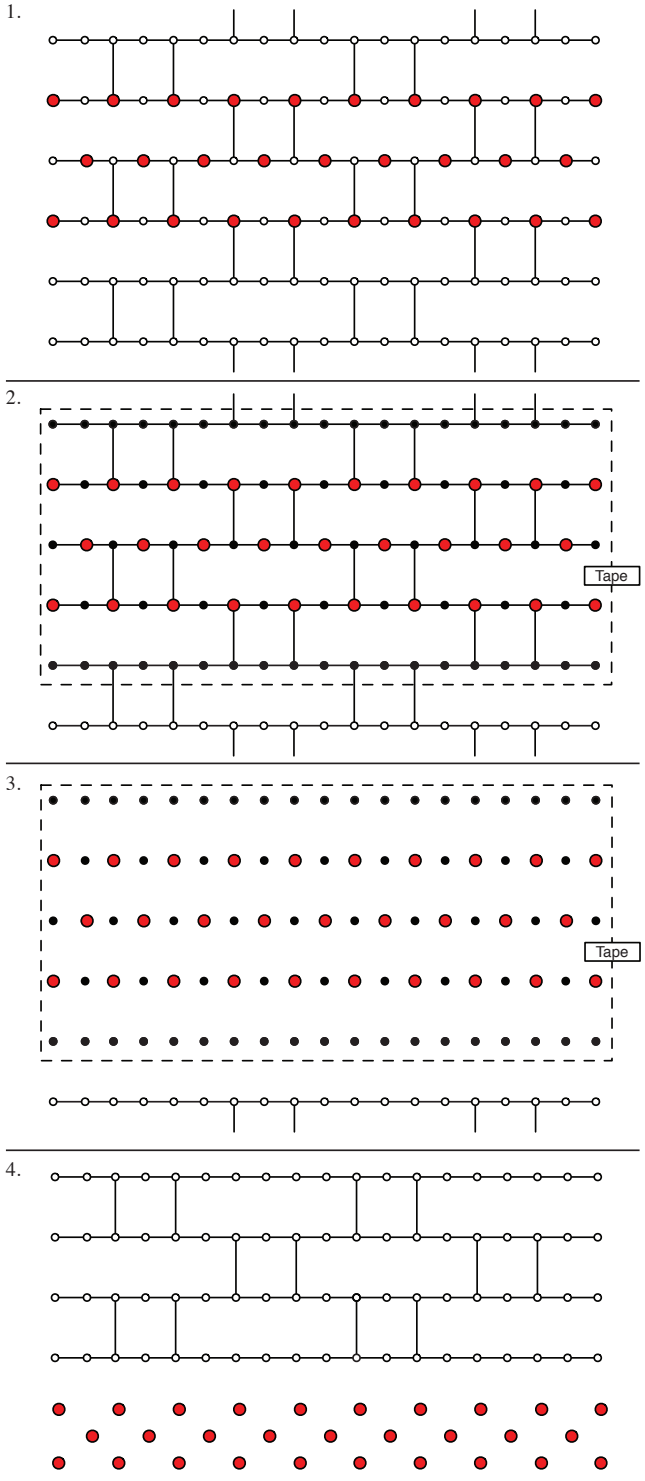

FIG. 4. Multi-trap verification on a cylindrical brickwork state: 1. Alice randomly selects a set of consecutive rows R and assigns trap qubits to every qubit in R corresponding to a random vertex colour in a two colouring of the graph. 2. The remaining qubits in the selected tape are dummy qubits and prepared in the computational basis. 3. Bob's entangling operation according to the cylindrical brickwork graph does not entangle the trap qubits to the rest of the brickwork state. 4. Discarding the dummy qubits, we finally obtain a tensor product of the brickwork state and the trap qubits.

leads to the following bound on the fidelity of the whole m-qubit input state

$$\begin{aligned} F(|\psi^B\rangle,\rho^B_{\rho_{\leq\tilde{\varepsilon}}}) &= \prod_{j=1}^{m} F\left(|\psi_j^B\rangle,\rho_j^B\right), \\ &\geq \left(1-\frac{1}{2}\tilde{\varepsilon}^2\right)^{2m}, \\ &\geq 1-m\tilde{\varepsilon}^2, \end{aligned}$$

where we take $\tilde{\varepsilon}$ to be the common upper bound on for all j. Using the relationship between trace distance and fidelity,

$$\frac{1}{2}\|\rho^B_{\leq\tilde{\varepsilon}}-|\psi^B\rangle\langle\psi^B|\|_{\mathrm{tr}} \leq \sqrt{1-F(|\psi^B\rangle,\rho^B_{\leq\tilde{\varepsilon}})},$$

it follows that

$$\|\rho^B_{\leq\tilde{\varepsilon}}-|\psi^B\rangle\langle\psi^B|\|_{\mathrm{tr}} \leq 2\sqrt{m}\tilde{\varepsilon}.$$

Therefore the total probability of Alice accepting an incorrect outcome is bounded by

$$\begin{aligned} p_{error} &\leq p(1-\Delta)+p\left\|\rho^B_{\leq\tilde{\varepsilon}}-|\psi^B\rangle\langle\psi^B|\right\|_{\mathrm{tr}}+(1-p) \\ &\leq 1-p\Delta+2p\sqrt{m}\tilde{\varepsilon}. \end{aligned} \tag{11}$$

Expanding the expression for Alice's confidence p and demanding that the confidence be close to unity, we obtain $\tilde{n}+m=\Theta(\varepsilon^{-2}\ln m)$. We would like to now find a scaling relationship between ε and the input size m. Requiring that the last term in Eq. (11) scale as a constant bounded from above by $p\Delta$ leads to $\tilde{\varepsilon}=O(m^{-1/2})$. Using Theorem 1 we know that $\tilde{\varepsilon}=O(\varepsilon^{1/4})$ which means that $\varepsilon=O(m^{-2})$. This finally leads to $\tilde{n}+m=O(m^4\ln m)$ which is the combined number of input qubits and the number of Bell pairs needed per measurement setting in the verification of remote state preparation. □

Conclusion

Our scheme offers a large improvement over current schemes [13, 15] that achieve a similar function. Splitting the computation into two parts, namely device-independent remote state preparation followed by authenticated computation, presents a distinct advantage. At all stages of phase one we only need to self-test individual EPR pairs, unlike the approach in [15] that self-tests the entire graph state. This results in the number of repetitions of their protocol to be $N \geq 3^{16}\cdot 10^{38.7}\cdot n^{22}$, where n is the number of vertices of the graph. It is worth noting that the client in [15] is completely classical and the protocol requires n non-communicating servers, each holding one vertex of the graph state. The protocol of Reichardt *et al.* [13] also considers a fully classical client and a constant number of non-communicating quantum servers. The client relies on CHSH games to test the shared states as well as the operation of the servers. To authenticate the whole computation, the client uses the servers to implement state and process tomography. This introduces a large overhead, where the leading term is of the order at least n^{8192}, where n counts the number of gates needed to implement the computation.

We note that in recent and independent work from the results reported here, Gheorghiu, Kashefi and Wallden have also considered splitting the verification problem into a remote state preparation followed by authenticated blind computation [27]. A major difference between their results and ours, is that their protocol utilizes the CHSH rigidity approach of [13], rather than Bell pair self-testing, resulting in overhead which scales as n^c for a constant $c > 2048$.

In contrast to these other methods, the protocol described here requires an overhead in resources that scales as $O(m^4 \ln m)$ where m is the number of vertices used in the computation. While this represents a drastic increase in efficiency over other existing schemes, further reducing overhead remains an important open question.

Acknowledgements

The authors acknowledge support from Singapore's National Research Foundation and Ministry of Education. This material is based on research funded by the Singapore National Research Foundation under NRF Award NRF-NRFF2013-01.

[1] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, and D. M. Lucas, "High-Fidelity Preparation, Gates, Memory, and Readout of a Trapped-Ion Quantum Bit," Phys. Rev. Lett. **113**, 220501 (2014).

[2] C. J. Ballance, T. P. Harty, N. M. Linke, and D. M. Lucas, "High-fidelity two-qubit quantum logic gates using trapped calcium-43 ions," (2014), arXiv:quant-ph/1406.5473 .

[3] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, "Superconducting quantum circuits at the surface code threshold for fault tolerance," Nature (London) **508**, 500–503 (2014).

[4] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on* (IEEE, 1994) pp. 124–134.

[5] S. Aaronson, "BQP and the polynomial hierarchy," in *Proceedings of the forty-second ACM symposium on Theory of computing* (ACM, 2010) pp. 141–150.

[6] D. Aharonov, M. Ben-Or, and E. Eban, "Interactive Proofs For Quantum Computations," in *Proceedings of Innovation in Computer Science* (Tsinghua University Press, 2010) p. 543.

[7] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on* (IEEE, 2009) pp. 517–526.

[8] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, "Composable security of delegated quantum computation," in *Advances in Cryptology–ASIACRYPT 2014* (Springer, 2014) pp. 406–425.

[9] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind computation," (2012), arXiv:quant-ph/1203.5217 .

[10] T. Morimae, "Verification for measurement-only blind quantum computing," Phys. Rev. A **89**, 060302 (2014).

[11] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," Science **335**, 303–308 (2012).

[12] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, "Experimental verification of quantum computation," Nature Physics **9**, 727–731 (2013).

[13] B. W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," Nature (London) **496**, 456–460 (2013).

[14] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," Phys. Rev. Lett. **23**, 880 (1969).

[15] M. McKague, "Interactive proofs for BQP via self-tested graph states," (2013), arXiv:quant-ph/1309.5675 .

[16] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Optimal blind quantum computation," Phys. Rev. Lett. **111**, 230502 (2013).

[17] T. Morimae and K. Fujii, "Secure entanglement distillation for double-server blind quantum computation," Phys. Rev. Lett. **111**, 020502 (2013).

[18] Y.-B. Sheng and L. Zhou, "Deterministic entanglement distillation for secure double-server blind quantum computation," Sci. Rep. **5**, 7815 (2015).

[19] T. Morimae and K. Fujii, "Blind quantum computation protocol in which alice only makes measurements," Phys. Rev. A **87**, 050301 (2013).

[20] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on* (IEEE, 1998) pp. 503–509.

[21] D. Mayers and A. Yao, "Self testing quantum apparatus," Quantum Inf. Comput. **4**, 273–286 (2004).

[22] M. McKague, T. H. Yang, and V. Scarani, "Robust self-testing of the singlet," J. Phys. A: Math. Theor. **45**, 455304 (2012).

[23] M. McKague and M. Mosca, "Generalized self-testing and the security of the 6-state protocol," in *Theory of Quantum Computation, Communication, and Cryptography* (Springer, 2011) pp. 113–130.

[24] S. Pironio, A. Acín, S. Massar, A. Boyer de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature (London) **464**, 1021–1024 (2010).

[25] W. Hoeffding, "Probability inequalities for sums of bounded random variables," J. Am. Stat. Assoc. **58**, 13–30 (1963).

[26] K. Azuma, "Weighted sums of certain dependent random variables," Tohoku Mathematical Journal, Second Series **19**, 357–367 (1967).

[27] A. Gheorghiu, E. Kashefi, and P. Wallden, "Robustness and device independence of verifiable blind quantum computing," New J. Phys. **17**, 083040 (2015).